PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-044354
(43)Date of publication of application : 14.02.1997

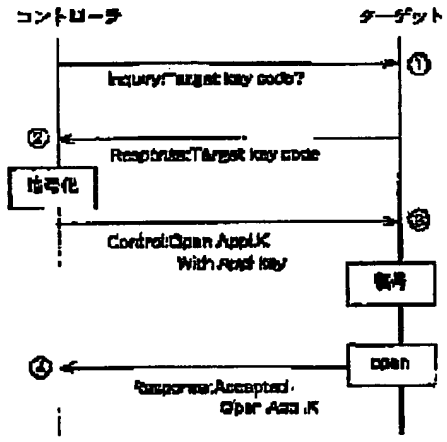
(51)Int.Cl. G06F 9/06
G06F 1/00
G06F 13/00
G09C 1/00
H04L 9/32
H04N 7/167

(21)Application number : 07-212633
(22)Date of filing : 28.07.1995

(71)Applicant : SONY CORP
(72)Inventor : KAWAMURA HARUMI

(54) ELECTRONIC APPARATUS AND ITS OPERATION CONTROL METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To enable other companies to use each independently developed application by transmitting a control signal, which includes preliminarily determined cipher information and has a prescribed format, from an apparatus on the control side and setting the application to the executable state by an apparatus on the controlled side in the case of reception of the control signal including preliminarily determined cipher information.
SOLUTION: When receiving a target key code from a target (2), a controller multiplies a cipher function by this target key code to calculate an application key code. An open command of the application to which the application number and the calculated application key code are added is transmitted to the target (3). The target confirms whether the decoded result is equal to its own target key code or not; and if it is equal, the target validates the open command of the application K and enters into the open state that the application can be executed.



LEGAL STATUS

[Date of request for examination] 29.07.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）

(12) 公開特許公報（A）

(11)特許出願公開番号

特開平9－44354

(43)公開日 平成9年(1997)2月14日

(51)Int.Cl.⁶		識別記号	庁内整理番号	FI		技術表示箇所
G06F	9/06	550		G06F	9/06	550G
	1/00	370			1/00	370E
	13/00	351	9460－5E		13/00	351F
G09C	1/00	660	7259－5J	G09C	1/00	660D
H04L	9/32			H04L	9/00	673Z

審査請求 未請求 請求項の数9 FD （全 10 頁） 最終頁に続く

(21)出願番号 特願平7－212633

(22)出願日 平成7年(1995)7月28日

(71)出願人 000002185
ソニー株式会社
東京都品川区北品川6丁目7番35号

(72)発明者 川村 晴美
東京都品川区北品川6丁目7番35号 ソニー株式会社内

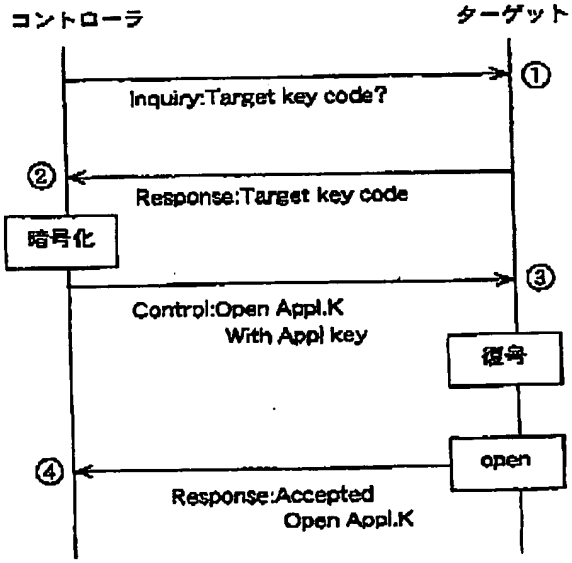
(74)代理人 弁理士 杉山 猛

(54)【発明の名称】 電子機器及びその動作制御方法

(57)【要約】

【課題】 ＩＥＥＥ－１３９４のベンダーユニークコマンドを用いて独自に開発したアプリケーション毎に他社による使用を可能にする。

【解決手段】 コントローラは、ターゲットキーコードを受けとると（手順②）、暗号関数とそのターゲットキーコードとから、アプリケーションキーコードを算出する。そして、アプリケーションキーコードを付けたアプリケーションのオープンコマンドを送信する（手順③）。ターゲットはオープンコマンドを受信したら、コマンド中のターゲットキーコードを復号する。そして、復号した結果が自分のターゲットキーコードと等しければ、アプリケーションを実行可能なオープン状態にする。



【特許請求の範囲】

【請求項１】 複数の電子機器をバスで接続し、該電子機器間で情報信号及び制御信号の通信を行なうシステムにおいて、電子機器の製造元情報を含む所定のフォーマットの制御信号を用いて実現したアプリケーションの動作を制御する方法であって、

制御する側の電子機器は制御される側の電子機器に対してあらかじめ定められた暗号情報を含む前記所定のフォーマットの制御信号を送信し、該制御される側の電子機器は受信した制御信号にあらかじめ定められた暗号情報が含まれていると共に、前記アプリケーションを実行可能状態にすることを特徴とする電子機器の動作制御方法。

【請求項２】 暗号情報は電子機器毎に定められているキーコードとアプリケーション毎に定められている暗号関数とから作成されるものである請求項１記載の電子機器の動作制御方法。

【請求項３】 制御する側の電子機器は制御される側の電子機器に対してキーコードを問い合わせ、該制御される側の電子機器から返答されたキーコードとあらかじめ自分が保持している暗号関数とから暗号情報を作成し、該暗号情報を前記制御される側の電子機器へ送信する請求項２記載の電子機器の動作制御方法。

【請求項４】 制御される側の電子機器は誤った暗号情報を受信してアプリケーションを実行可能状態にしなかったときに、アプリケーションを実行可能状態にしたことを制御する側の電子機器に知らせる請求項１記載の電子機器の動作制御方法。

【請求項５】 制御する側の電子機器は制御される側の電子機器に対して製造元情報を問い合わせ、該制御される側の電子機器から返答された製造元情報があらかじめ自分が保持しているリストに登録されているかどうかを判定し、登録されていないときは、アプリケーションを実行可能状態にする手順を実行しない請求項１記載の電子機器のアプリケーションの動作制御方法。

【請求項６】 キーコードをあらかじめ定められた期間毎に変化させる請求項２記載の電子機器の動作制御方法。

【請求項７】 キーコードをあらかじめ定められた生産台数毎に変化させる請求項２記載の電子機器の動作制御方法。

【請求項８】 キーコードと暗号情報とを１対１に割り付けた請求項２記載の電子機器の動作制御方法。

【請求項９】 複数の電子機器をバスで接続し、該電子機器間で情報信号及び制御信号の通信を行なうシステムにおける電子機器であって、

電子機器の製造元を示す識別情報を含む所定のフォーマットの制御信号を用いて実現したアプリケーションを有し、あらかじめ定められた暗号情報が含まれている所定のフォーマットの制御信号により前記アプリケーションを実行可能状態にすることを特徴とする電子機器。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は複数の電子機器をバスで接続し、それらの電子機器間で通信を行なうシステムに関し、より詳細には独自に開発したアプリケーションをライセンス契約して他社でも使用可能とするためのシステムに関する。

【０００２】

【従来の技術】複数の電子機器をバスで接続し、それらの電子機器間で通信を行なうシステムとしては、ＩＥＥＥ－１３９４シリアルバスを用いた通信システムが考えられている。ＩＥＥＥ－１３９４シリアルバスを用いた通信システムは、デジタルビデオテープレコーダ、デジタルビデオカメラ、デジタルテレビジョン受像機、パーソナルコンピュータ等の電子機器（以下機器と略す）をＩＥＥＥ－１３９４シリアルバスで接続し、それらの機器間でデジタルオーディオ／ビデオ信号等の情報信号や接続制御コマンド等の制御信号の通信を行なうものである。

【０００３】ＩＥＥＥ－１３９４シリアルバスを用いた通信システムでは、各メーカーが独自のアプリケーションを実現するためにベンダーユニークコマンド（Ｖｅｎｄｏｒ Ｕｎｉｑｕｅ Ｃｏｍｍａｎｄ）が用意されている（各社で互換性をとるべき基本的なコマンドはベンダーユニークコマンドとは別に定義されている。）。ベンダーユニークコマンドのパケットには、そのメーカーであることを示すカンパニーＩＤを付けることになっている。したがって、基本的にベンダーユニークコマンド用いて実現するアプリケーションは、そのメーカー１社でのみ有効となるものである。

【０００４】

【発明が解決しようとする課題】独自に開発されたアプリケーションであっても他社に有効な場合がある。そのアプリケーションが共通コマンドとして登録するほどの汎用性がない場合には、あるメーカーが開発したアプリケーション用のコマンドを他のメーカーでも使用したいことがある。他のメーカーがそのアプリケーション用のベンダーユニークコマンドを使用するには、アプリケーションを開発したメーカーのカンパニーＩＤを使用しなければならない。

【０００５】そこで、アプリケーションを開発したメーカーが正式にライセンス契約をして他のメーカーにカンパニーＩＤの使用を認めたとすると、そのアプリケーション以外のベンダーユニークコマンドまでもが他社でも使用できてしまう。

【０００６】本発明はこのような問題点に鑑みてなされたものであって、独自に開発したアプリケーション毎に他社による使用を可能にする機器及びその制御方法を提供するものである。

【0007】
【課題を解決するための手段】前記課題を解決するために、本発明に係る機器及びその動作制御方法は、複数の機器をバスで接続し、これらの機器間で情報信号及び制御信号の通信を行なうシステムにおいて、機器の製造元を示す識別情報を含む所定のフォーマットの制御信号を用いて実現したアプリケーションの動作を制御する方法であって、制御する側の機器は制御される側の機器に対してあらかじめ定められた暗号情報を含む前記所定のフォーマットの制御信号を送信し、制御される側の機器は受信した制御信号にあらかじめ定められた暗号情報が含まれているときに、前記アプリケーションを実行可能状態にすることを特徴とするものである。
【0008】本発明によれば、制御する側の機器は制御される側の機器に対してあらかじめ定められた暗号情報を含む前記所定のフォーマットの制御信号を送信し、制御される側の機器は受信した制御信号にあらかじめ定められた暗号情報が含まれているときに、前記アプリケーションを実行可能状態にする。
【0009】
【発明の実施の形態】以下本発明の実施の形態について、
〔1〕ベンダーユニークコマンド（Ｖｅｎｄｏｒ Ｕｎｉｑｕｅ Ｃｏｍｍａｎｄ）
〔2〕ベンダーユニークコマンドの他社での使用
【0010】〔3〕システムの内容説明
（3－1）アプリケーションのオープン
（3－2）暗号化の条件
（3－3）アプリケーションのオープンに必要な情報
（3－4）アプリケーションのオープンの方法
（3－5）オープン中のコマンド
（3－6）アプリケーションのクローズ
（3－7）アプリケーション実行およびクローズの条件
【0011】〔4〕アプリケーションの保護
（4－1）カンパニーＩＤによる管理
（4－2）ターゲットキーコードの設定
（4－3）暗号関数ｆｋ
【0012】〔5〕ターゲットの構成と動作
の順序で詳細に説明する。
【0013】〔1〕ベンダーユニークコマンド（Ｖｅｎｄｏｒ Ｕｎｉｑｕｅ Ｃｏｍｍａｎｄ）
ＩＥＥＥ－１３９４シリアルバスに対するデジタルインターフェイスの機能制御プロトコル（Ｆｕｎｃｔｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ：以下ＦＣＰと略す）では、複数のコマンドトランザクションセット（ＣｏｍｍａｎｄＴｒａｎｓａｃｔｉｏｎ Ｓｅｔ）を使用することができる。
【0014】図１にベンダーユニークフレームのフォーマットを示す。ここで、ＣＴＳ（Ｃｏｍｍａｎｄ Ｔｒａｎｓａｃｔｉｏｎ Ｓｅｔ）＝１１１０がベンダーユニークフレームであることを示す。そして、ＣＴＳの次に４ビットを空けて、３バイトのベンダーＩＤ（ＩＥＥＥで定められたカンパニーＩＤ）を用いる。ベンダーユニークであることを示すＣＴＳとベンダーＩＤ以外はベンダーが自由に定義し、使用することができる。つまり、そこで使用するコマンドセットもコマンド／レスポンスの送受信等のトランザクションについてもベンダーに依存することとなっている。なお、ゼロパッドバイト（ｚｅｒｏ ｐａｄ ｂｙｔｅｓ）は、フレームの長さを４バイト（クアドレット）単位にするために必要に応じて設けられる。
【0015】図２にＡＶ機器制御用のコマンドトランザクションセットであるＡＶ／Ｃ（Ａｕｄｉｏ Ｖｉｓｕａｌ／Ｃｏｎｔｒｏｌ）コマンドトランザクションセットのフレーム構成を示す。ここで、ＣＴＳ＝０００００がＡＶ／Ｃコマンドトランザクションセットであることを示す。
【0016】ＡＶ／Ｃコマンドトランザクションセットでも、ベンダーが自由にコマンドを定義することができるようにオペコード（ＯＰＣ）としてベンダーユニークが定義されている。ただしコマンド／レスポンスのトランザクションについてはＡＶ／Ｃコマンドトランザクションセットに従う。この場合のフレーム構成を図３に示す。ＯＰＣ＝００ｈでベンダーユニークであることを表す。ベンダーＩＤは前記の場合と同様、３バイトのカンパニーＩＤを用いる。
【0017】〔2〕ベンダーユニークコマンドの他社での使用
ＦＣＰでは他のノードを制御するノードのことをコントローラ、制御される側のノードをターゲットと呼ぶ。以下コントローラ、ターゲットという名称を用いて説明する。
【0018】ベンダーユニークコマンドはベンダーＩＤに記されたカンパニーＩＤを所有している会社が定義し、使用するものであるが、アプリケーションによっては他の会社も同じコマンドを使用したい場合も出てくる。
【0019】ここではカンパニーＩＤ＝ｘｘｘｘｘｘｈのＡ社と、カンパニーＩＤ＝ｙｙｙｙｙｙｈのＢ社を例に説明する。Ａ社はアプリケーションＫの独自のコマンドをベンダーユニークコマンドとして定義し、Ａ社の製品で使用している。Ｂ社はＡ社のこのベンダーユニークコマンドを用いたアプリケーションＫをＢ社の製品でも対応したいと考えた。Ｂ社での対応の方法としては２つの場合がある。Ｂ社がコントローラを製造しＡ社の製品をターゲットとして制御する場合と、Ｂ社がターゲットとなる製品を作りＡ社のコントローラで制御されるようにする場合である。どちらの場合でもＡ社のベンダーユニークコマンドを使用しなければアプリケーションＫの実現はできない。

【００２０】以下に説明するシステムは、ベンダーユニークコマンドの所有者である会社がベンダーユニークコマンドを用いて実現したアプリケーションのうち幾つかについては、限定した会社での使用を可能とするためのものである

【００２１】このシステムを導入することによって、一般的にはベンダーユニークコマンドの他社での使用を禁止とするが、アプリケーション毎に使用権を与えるようにすることが可能となる。したがって前記の場合のＢ社もＡ社のアプリケーションＫに関してはベンダーユニークコマンドを使用することができるようになる。

【００２２】〔３〕システムの内容説明

（３－１）アプリケーションのオープン

ターゲットはベンダーユニークコマンドにより実現するアプリケーション毎に、「オープン状態」「クローズ状態」を有する。オープン状態とはコマンドを受けて、そのアプリケーションを実行することが可能な状態である。クローズ状態とは、コマンドを受けたとしても実行しない状態である。

【００２３】前記のようにベンダーユニークコマンドは一般に公開しているコマンドではないので、第三者（Ｃ社とする）が勝手にＡ社のカンパニーＩＤ＝ｘｘｘｘｘｘｈを付けてコマンドを送った場合にコマンドが実行されないようにするため、通常はアプリケーションを全てクローズ状態にしておく。そして、ベンダーユニークコマンドを定義したＡ社はもとより、使用権を得たＢ社についても、該当するアプリケーションＫをオープン状態にしてからアプリケーションＫを実行することとした。このとき、オープン状態にするための手段を教えることがそのアプリケーションの使用権を与えることに等しい。

【００２４】（３－２）暗号化の条件

コントローラはターゲットに対して、オープン状態にしたいアプリケーションを指定してオープンコマンドを送る。この時、コントローラとターゲットの間で取り決めを交わしておき、決められたコードを付けてオープンコマンドが送られた場合のみ有効とする。このコードは第三者にはわからないようにする必要がある。このコードは、あらかじめＡ社とＢ社との間で決めておく。そのとき、各機器毎あるいは１つの機器でも時間によって異なる値にするなどの対応をとる。

【００２５】このコードは一種の暗号と考えられるが、コンスーマー機器での使用を目的とするので、１チップマイクロコンピュータでも簡単に対応できるようにし、コントローラ、ターゲット共に負担をできるだけ軽くする必要がある。コンスーマー機器では商品が一度市場に出たならば、その後暗号の方式を変えることは困難である。

【００２６】（３－３）アプリケーションのオープンに必要な情報

各アプリケーションをオープンさせる際に必要な情報について説明する。

（１）アプリケーションナンバー（Ａｐｐｌｉｃａｔｉｏｎ Ｎｏ）

アプリケーションの種別をあらわすコードをアプリケーションナンバーと呼ぶことにする。図４にアプリケーションナンバーの例を示す。ここでは、１バイトでアプリケーションの種類を表している。アプリケーションナンバーを０１ｈからＦＥｈまで割り当て可能とすると、２５４種類のアプリケーションまで対応できる。００ｈは各アプリケーションに共通に用いるために使用禁止（ｒｅｓｅｒｖｅｄ）としておく。また、アプリケーションの数が増えた時のために、ＦＦｈは拡張用としてｒｅｓｅｒｖｅｄとしておく。

【００２７】（２）暗号関数ｆ

アプリケーションをオープンさせる際にアプリケーションナンバーとともに送る「鍵」をアプリケーションキーコードと呼ぶ。アプリケーションキーコードの生成方法（暗号化）はアプリケーション毎に異なり、あらかじめＡ社、Ｂ社間で決めておく。これを暗号関数ｆとし、アプリケーションＫの暗号関数をｆｋとする。

【００２８】（３）ターゲットキーコード

ターゲットキーコードはターゲット毎に定める値であり、全てのアプリケーションに対してアプリケーションキーコードの生成の元となるものである。そして、機器毎に異なるターゲットキーコードを付ける等の対応によって、１つのアプリケーションでもアプリケーションキーコードを変える。

【００２９】アプリケーションのオープンの際には、コントローラはターゲットにターゲットキーコードの問い合わせ命令を送り、返答を得ることにより、その時のターゲットキーコードを知る。

【００３０】（４）アプリケーションキーコード

ターゲットキーコードを暗号関数ｆで暗号化したものがアプリケーションキーコードとなる。つまり、アプリケーションＫに対するアプリケーションキーコードは

アプリケーションキーコード＝ｆｋ（ターゲットキーコード）

と表せる。

【００３１】（３－４）アプリケーションのオープンの方法

コントローラがターゲットのアプリケーションＫをオープン状態にする方法について説明する。

【００３２】（１） コマンド送信手順

図５にコントローラ／ターゲット間のコマンド／レスポンスの概略図を示す。まず、コントローラはターゲットに対し、ターゲットキーコードの問い合わせコマンドを送信する（手順①）。ターゲットはそれに対するレスポンスとして、その時の自分のターゲットキーコードを返信する（手順②）。

【００３３】コントローラは、ターゲットキーコードを受けとると、暗号関数ｆｋにそのターゲットキーコードをかけ、アプリケーションキーコードを算出する。次に、コントローラはターゲットに対し、アプリケーションＮｏと算出したアプリケーションキーコードを付けて、アプリケーションのオープンコマンドを送信する（手順③）。

【００３４】ターゲットはオープンコマンドを受信したら、指定されたアプリケーションＮｏのアプリケーションを備えているかどうかを確認する。そして、対応しているアプリケーションの場合、受信したアプリケーションキーコードをその暗号関数ｆｋの逆関数にかけ、復号する。

【００３５】ターゲットは復号した結果が自分のターゲットキーコードと等しいかどうか確認する。そして、等しい場合に初めてアプリケーションＫのオープンコマンドを有効とし、アプリケーション実行可能なオープン状態に入る。

【００３６】ターゲットはアプリケーションＫをオープン状態にしたら、コントローラに対して、アプリケーションＫをオープン状態にしたこと知らせるためのレスポンスを返す（手順④）。

【００３７】（２）コマンドフォーマット

図１と図３を参照しながら説明したように、ベンダーユニークコマンドは、ベンダーユニークフレーム又はＡＶ／Ｃコマンドトランザクションセットのいずれを用いても実現できるが、ここでは、コマンド構成として、ＡＶ／Ｃコマンドトランザクションセットを用いた場合の例を示す。

【００３８】図６にベンダーユニークコマンドの構成を示す。ここでは３バイトのベンダーＩＤに続くベンダーが独自に定義する領域（ＯＰＲ４以降）のみ図示した。前述したように、コマンド／レスポンスのトランザクションについてはＡＶ／Ｃコマンドトランザクションセットに準ずるものとする。アプリケーションを実行する具体的なコマンドについてはここで記載しない。これは各アプリケーン毎に定義する。

【００３９】図７にターゲットキーコードの問い合わせのコマンド／レスポンスを示す。ここではアプリケーションＮｏをｋｋｈ、ターゲットキーコードを１６ビットの１２３４ｈとした。なお、ターゲットキーコードの長さはアプリケーション毎に定めることができる。

【００４０】ターゲットキーコードは機器毎／アプリケーション毎に異なる値としたり、乱数とすることも考えられるので、各アプリケーションを実行開始する際には必ず問い合わせをする。図７（ａ）は問い合わせのコマンドを示す。ここでＯＰＲ４はアプリケーションＮｏであり、ＯＰ５の１０ｈとＯＰ６の７１ｈでターゲットキーコードの問い合わせであることを示す。また、ＯＰ７とＯＰ８はＦＦｈ（ダミー）とする。

【００４１】ターゲットは、問い合わせのコマンドに付いているアプリケーション（アプリケーションＫ）に対応している場合には、図７（ｂ）に示すように、ＯＰ７とＯＰ８に１６ビットのターゲットキーコード１２３４ｈを付けた“Ｓｔａｂｌｅ”のレスポンスをコントローラに返答する。そのアプリケーションに対応していない場合には、図７（ｃ）に示すように、問い合わせコマンドと同じ内容の“Ｎｏｔ　Ｉｍｐｌｅｍｅｎｔｅｄ”のレスポンスを返す。

【００４２】次に、コントローラがターゲットに送るアプリケーションＫのオープンコントロールコマンドおよびそのレスポンスを図８（ａ），（ｂ）に示す。ここではアプリケーションキーコードを１６ビットの５６７８ｈとした。なお、アプリケーションキーコードの長さはアプリケーション毎に定めることができる。

【００４３】コマンドに付いているアプリケーションキーコードの指定値がターゲットが持っているアプリケーションキーコードの値と異なっていてオープンできない場合には、コントローラに対して“Ｒｅｊｅｃｔｅｄ”のレスポンスを返すのが基本である。しかし、第三者がアプリケーションキーコード捜し求める過程においては、０００ｈからＦＦＦＦｈまで１つづつ試してみるということが考えられる。そこでオープンできなかった場合でもわざと“Ａｃｃｅｐｔｅｄ”のレスポンスを返答する。図８（ｃ），（ｄ）にオープンできない場合の例（正しいアプリケーションキーコード＝５６７８ｈのところ、５６７９ｈを指定）を示す。第三者はオープンコマンドのトランザクションだけではオープンに成功したかどうかわからないので、アプリケーションの実行コマンドを送ってみるか、オープン中かどうか問い合わせて調べるという手順が必要となる。

【００４４】アプリケーションがオープン状態であるかクローズ状態であるかの問い合わせもアプリケーションキーコードを付けて送る。アプリケーションキーコードの指定値が正しい場合には“Ａｃｃｅｐｔｅｄ”を、異なっている場合には“Ｒｅｊｅｃｔｅｄ”をレスポンスとして返す。図９（ａ），（ｂ）にアプリケーションキーコードとして正しい値（５６７８ｈ）を指定された場合のコマンドとレスポンスの例を示す。

【００４５】（３－５）オープン中のコマンド

アプリケーションがオープン（実行可能状態）している間のみ、ターゲットはそのアプリケーション用のコマンドを受け付ける。コマンドフォーマットとしては図６のように最初の１バイトでアプリケーションＮｏを示す他は、各アプリケーション毎に定める。

【００４６】アプリケーションがオープン状態であるか、クローズ状態であるかにかかわらず、対応していないアプリケーションの実行コマンドを受けた場合にはレスポンスとしては“Ｎｏｔ　Ｉｍｐｌｅｍｅｎｔｅｄ”を返す。また、アプリケーションがオープン状態であっ

ても、アプリケーション毎に定めたＯＰＯとして指定されたものに対応していない場合には、レスポンスとしては“Ｎｏｔ Ｉｍｐｌｅｍｅｎｔｅｄ”を返す。

【００４７】（３－６）アプリケーションのクローズ

ターゲットとなる機器は電源をオフにする際に基本的に全てのアプリケーションを自動的にクローズ状態にする。再び電源が入れられた場合にもクローズ状態を継続する。

【００４８】コントローラはアプリケーションの実行を終了した際に、ターゲットにクローズコマントを送信する。図１０にクローズコマンドの例を示す。このように、クローズの際にもアプリケーションキーコードを付けてコマンドを送る。ターゲットはクローズコマンドを受けとると、そのクローズコマンドのアプリケーションＮｏに示されるアプリケーションをクローズ状態にする。このとき、アプリケーションキーコードの値が異なっていてもクローズ状態にする。本システムでは通常はアプリケーションはクローズ状態とし、実行させる際のみにオープンさせることが基本である。

【００４９】なお、オープン状態ならば受け付けるコマンドをクローズ状態で受けた場合には、レスポンスとしては“Ｒｅｊｅｃｔｅｄ”を返す。

【００５０】（３－７）アプリケーション実行およびクローズの条件

アプリケーションによっては長時間オープンのままでは問題が生じるものや、一度オープンさせたら独占的に制御を行ないたいものなど、様々な場合が考えられる。したがって、アプリケーション毎にその用途に適した実行条件等を定めるものとする。以下にその例を記す。

【００５１】（１）オープン時間の制限

オープン状態にいるにもかかわらず、そのアプリケーション実行のためのコマンドが一定時間以上アクセスされない場合には、強制的にクローズする。タイムアウトの時間についてはアプリケーション毎に定める。

【００５２】（２）バスの異常処理

バスにリセットがかかった場合には、強制的にクローズする。

【００５３】（３）アプリケーション実行許可台数

複数のコントローラからの制御を許可しないようにする。ターゲットはそのアプリケーションをオープンしたコントローラを記憶しておき、アプリケーショ実行コマンドについてはそのコントローラからのコマンドのみ受けるようにする。このとき、オープン中であっても他のコントローラからのコマンドはＲｅｊｅｃｔする。複数のコントローラからの制御を許可するが、その台数を限定してもよい。

【００５４】〔４〕アプリケーションの保護

暗号化したアプリケーションキーコードを送るからといっても、そのアプリケーションを完璧に保護したことにはならない。このアプリケーションの使用権を持たない第三者であっても、コントローラとターゲットの間の通信内容は傍受できるので、傍受したターゲットキーコードとアプリケーションキーコードからコンピュータを用いて暗号関数ｆｋを求めることが考えられるからである。

【００５５】（４－１）カンパニーＩＤによる管理

そこで、このような事態に対してアプリケーションを保護する手段を考えた。使用権を持たない第三者がターゲットとなる機器を作った場合、コントローラ側の負荷を無視すれば、以下のような方法で第三者の検出を行ないアプリケーションを実行させないことが可能である。

【００５６】パーソナルコンピュータがコントローラとなり、アプリケーションを実行させるような場合の例を説明する。パーソナルコンピュータにアプリケーション実行の対象となる会社（使用権を持っている会社）のカンパニーＩＤを登録しておく。そして、ターゲットにベンダーＩＤの問い合わせコマンドを送り、そのレスポンスに付けられたベンダーＩＤが登録されているかどうかを調べる。ＩＥＥＥ－１３９４シリアルバスに対応する機器は、内部にノードユニークＩＤが書き込まれているので、例えば図５の手順①より前にこの問い合わせを行なう。このとき、第三者であるＣ社（カンパニーＩＤ＝ｚｚｚｚｚｚｈ）が、勝手にＡ社のベンダーＩＤ＝ｘｘｘｘｘｈに基づくベンダーユニークコマンド受けアプリケーションＫを実行できるように作ったとしても、コントローラは図１１に示すような登録ＩＤのリストを基に、Ｃ社が登録されていないことを知ることができるので、アプリケーションＫを起動させないようにすることができる。

【００５７】この場合、実際にはアプリケーションＫの使用権を得る会社が増えることが考えられるので、上記例のような保護の仕方は、リストの更新が可能となるような場合に適用できるものである。

【００５８】（４－２）ターゲットキーコードの設定

アプリケーションキーコード＝ｆｋ（ターゲットキーコード）

の関係式では、ターゲットキーコード，アプリケーションキーコードのサンプル数が多いほど、暗号関数ｆｋの解読は容易となる。コンスーマー機器での適用を考えると、ある機種においてターゲットキーコードが頻繁にではなくたまに変化することが望ましい。そこで、例えば以下のようにターゲットキーコードの設定を行なう。

【００５９】（１）生産台数での切替え

例えば１０万台ごとにターゲットキーコードを切り替える。第三者がコントローラを作った場合、最初の１０万台のターゲットキーコードには対応できても、その後生産されたものについては第三者の作ったコントローラでは動作しないことになる。

【００６０】（２）内蔵時計（カレンダー）での切替え

同一機器でも、例えば１年ごとにターゲットキーコード

を切り替える。１９９５年に生産された機器は１９９５をもとにした値をターゲットキーコードとする。第三者はこの初期のターゲットキーコードをもとにコントローラを作ることになる。したがって、当初は第三者のコントローラでも動作してしまうが、年が変わると動作しなくなる。

【００６１】（４－３）暗号関数ｆｋ

暗号関数ｆｋが数値演算式の場合、ターゲットキーコード，アプリケーションキーコードのサンプル数によっては簡単にｆｋを求めることができる。そこでコンスーマー機器への導入の際には、ｆｋは数値関数とはせず、ターゲットキーコードに対してアプリケーションキーコードを１対１に割り付け、その対応表をｆｋとしてアプリケーションＫの使用権を持つ会社にも渡すこととする。図１２に対応表の例を示す。このようにすれば、暗号関数ｆｋを求めることは困難になる。また、１チップマイクロコンピュータでも簡単に対応できる。さらに、商品が一度市場に出た後でも、ＲＯＭのバージョンアップにより比較的簡単に暗号の方式を変えることができる。

【００６２】〔５〕ターゲットの構成

図１３に本発明を適用したターゲットの構成の例を示す。この図に示すように、ターゲットとなるノードは、マイクロコンピュータ１と、ターゲットキーコードメモリ２と、暗号関数メモリ３と、時計４と、通信インターフェイス５とを備えている。

【００６３】マイクロコンピュータ１は内蔵するアプリケーションのオープン／クローズ、コマンド／レスポンスの作成、アプリケーションキーコードの作成等、アプリケーションに関する処理の全てを司る。

【００６４】ターゲットキーコードメモリ２は、アプリケーション毎に異なるターゲットキーコードを保持している。また、ここにはターゲットキーコードを１年毎に切り替えられるように、各アプリケーション毎に複数のターゲットキーコードが格納されている。

【００６５】暗号関数メモリ３はアプリケーション毎の暗号関数ｆｋを保持している。ここでは、図１２のようなターゲットキーコードとアプリケーションキーコードとの対応表を記憶したＲＯＭテーブルである。

【００６６】時計４は現在の時刻情報をマイクロコンピュータ１に知らせる。マイクロコンピュータ１はこの時刻情報を見て、年が変わるごとにターゲットキーコードを切り替えて読み出す。

【００６７】通信インターフェイス５はＩＥＥＥ－１３９４シリアルバス６に対してコマンド／レスポンスを送受信するためのインターフェイスである。なお、実際のターゲットにはオーディオ／ビデオ信号を処理するためのブロックが設けられているが、ここではアプリケーションのオープンに関連するブロックのみを示した。

【００６８】ここでコントローラの構成について簡単に説明しておく。図１３のターゲットに対応するコントローラは、マイクロコンピュータと、暗号関数メモリと、通信インターフェイスを備えている。もしコントローラが、（４－１）で説明したカンパニーＩＤによる管理を行なっているのであれば、さらにアプリケーション実行の対象となる会社カンパニーＩＤを登録しておくメモリを備えている。

【００６９】次に図１３に示したターゲットがアプリケーションをオープンにするまでの動作を説明する。まず、コントローラが送信したターゲットキーコードの問い合わせコマンドを受けとる（図５の手順①、図７（ａ）を参照）。マイクロコンピュータ１はターゲットキーコードメモリ２を参照し、問い合わせコマンドに付いていたアプリケーションＮｏに対応するターゲットキーコードを読み出し、通信インターフェイス５を介して“Ｓｔａｂｌｅ”のレスポンスを送信する（図５の手順②、図７（ｂ）を参照）。問い合わせコマンドに付いていたアプリケーションＮｏに対応するターゲットキーコードが存在しない場合には、“Ｎｏｔ Ｉｍｐｌｅｍｅｎｔｅｄ”のレスポンスを送信する（図７（ｃ）を参照）。

【００７０】コントローラはターゲットから“Ｓｔａｂｌｅ”のレスポンスを受けとると、そこに付いているターゲットキーコードを抽出し、内蔵する暗号関数メモリを読み出してアプリケーションキーコードを作成する。この暗号関数メモリはターゲットの暗号関数メモリ３と同様に構成されている。コントローラは作成したアプリケーションキーコードを付けたオープンコマンドをターゲットに送信する。（図５の手順③、図８（ａ）を参照）。

【００７１】ターゲット内のマイクロコンピュータ１は、受けとったオープンコマンドに付いていたアプリケーションキーコードと、自分の暗号関数メモリ３に格納されているターゲットキーコードに対応するアプリケーションキーコードとを比較する。すなわち、ここでは図５に示したように暗号関数の逆関数を用いてアプリケーションキーコードからターゲットキーコードを復号化するのではなく、コントローラと同様、暗号化を行なっているわけである。勿論、アプリケーションキーコードからターゲットキーコードを復号するように構成してもよい。比較したアプリケーションキーコード同士が一致していれば、アプリケーションをオープン状態にすると共に、コントローラに対して、アプリケーションをオープン状態にしたこと知らせるため“Ａｃｃｅｐｔｅｄ”のレスポンスを返す（図５の手順④を参照）。

【００７２】

【発明の効果】以上詳細に説明したように、本発明によれば機器の製造元を示す識別情報を含む所定のフォーマットの制御信号を用いた独自のアプリケーションを他社でも使用することができ、かつアプリケーション毎に使用を許可／禁止することができる。そして、複雑な暗号

化等を用いずにアプリケーションの保護が可能となる。

【図面の簡単な説明】

【図1】ベンダーユニークフレームのフォーマットを示す図である。

【図2】AV／Cコマンドトランザクションセットのフレーム構成を示す図である。

【図3】AV／Cコマンドトランザクションセットで定義されているベンダーユニークフレームの構成を示す図である。

【図4】アプリケーションナンバーの例を示す図である。

【図5】コントローラ／ターゲット間のコマンド／レスポンスの概略を示す図である。

【図6】ベンダーユニークコマンドの構成を示す図である。

【図7】ターゲットキーコードの問い合わせのコマンド／レスポンスを示す図である。

【図8】アプリケーションKのオープンコントロールコマンド／レスポンスを示す図である。

【図9】アプリケーションキーコードとして正しい値を指定された場合のオープン／クローズ問い合わせコマンド／レスポンスの例を示す図である。

【図10】クローズコマンドの例を示す図である。

【図11】使用権を持っている会社のカンパニーIDの登録リストの例を示す図である。

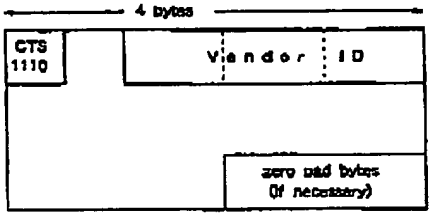
【図12】ターゲットキーコードとアプリケーションキーコードの対応表の例を示す図である。

【図13】ターゲットの構成の例を示す図である。

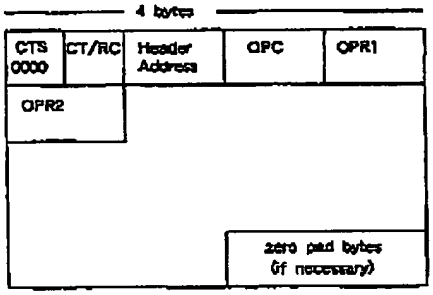
【符号の説明】

1…マイクロコンピュータ、2…ターゲットキーコードメモリ、3…暗号関数メモリ、4…時計、5…通信インターフェイス、6…IEEE－1394シリアルバス

【図1】

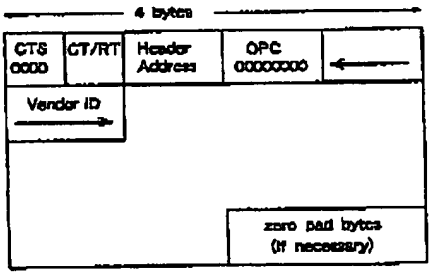


【図2】



CTS:コマンドトランザクションセット
CT/RC:コマンドタイプ／レスポンスタイプ
Header Address:コマンドの宛先、レスポンスの発信元のサブデバイス(あるいはデバイス)
OPC:オペコード
OPR:オペランド

【図3】



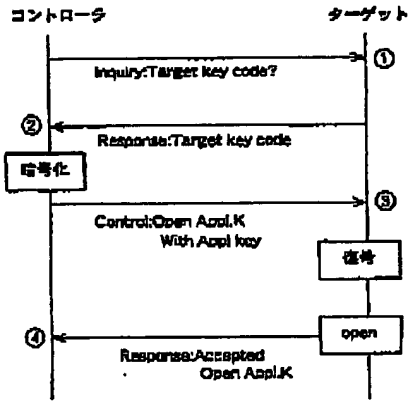
【図4】

Application No	アプリケーションの種類
00 h	(使用禁止)
01 h	VCR制御（基本）
02 h	VCR制御（特殊）
03 h	チューナー制御
：	：
10 h	録画情報
：	：
kk h	アプリケーションK
：	：
FE h	：
FF h	(reserved)

【図10】

kk h (Appl. K)	60 h (open/close)	00 h (close)	56 h (Application key code)	76 h

【図5】



【図6】

OPR4	OPR5	OPR6	OPR7	
Application No	Application 毎に定めた OPC	Application 毎に定めた OPR1	Application 毎に定めた OPR2	..

【図7】

OPR4	OPR5	OPR6	OPR7	OPR8
kk h (Appl. K)	10 h (Target key)	71 h (Value Inq)	FF h (dummy)	FF h (dummy)

(a) Status Inquiry Command

kk h (Appl. K)	10 h (Target key)	71 h (Value Inq)	12 h (Target key code)	34 h

(b) Response Stable

kk h (Appl. K)	10 h (Target key)	71 h (Value Inq)	FF h (dummy)	FF h (dummy)

(c) Response Not Implemented

【図8】

kk h (Appl. K)	60 h (open/close)	01 h (open)	56 h (Application key code)	78 h

(a) Control Command

kk h (Appl. K)	60 h (open/close)	01 h (open)	56 h (Application key code)	78 h

(b) Response Accepted

kk h (Appl. K)	60 h (open/close)	01 h (open)	56 h (Application key code)	78 h

(c) Control Command

kk h (Appl. K)	60 h (open/close)	01 h (open)	56 h (Application key code)	78 h

(d) Response Accepted

【図9】

kk h (Appl. K)	60 h (open/close)	FF h (dummy)	56 h (Application key code)	78 h

(a) Status Inquiry Command

kk h (Appl. K)	60 h (open/close)	01 h (open)	56 h (Application key code)	78 h

(b) Response Accepted

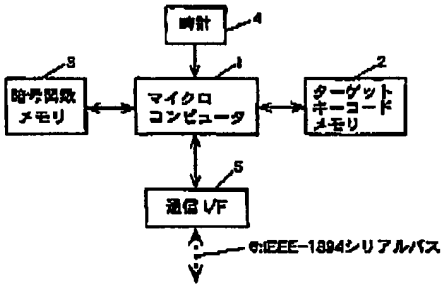
【図11】

Application No	使用権を持っている会社のCompany id
1	xxxxxxh
2	xxxxxxh, yyyyyyh
:	:
K	xxxxxxh, yyyyyyh
:	

【図12】

Target key code	Application key code
1234 h	5678 h
0088 h	0041 h
3333 h	8899 h
:	:

【図13】



フロントページの続き

(51) Int. Cl.⁶	識別記号	庁内整理番号	F I		技術表示箇所
H04N 7/167			H04N 7/167	Z	